Contents

System Security

Analyzing Android Repackaged Malware by Decoupling Their Event Behaviors ........................................ 3
Zimin Lin, Rui Wang, Xiaqi Jia, Shengzhi Zhang, and Chuankun Wu

Hybrid Risk Assessment Model Based on Bayesian Networks ............... 21
François-Xavier Aguessy, Olivier Bettan, Gregory Blanc, Vania Conan, and Hervé Debar

Hooking Graceful Moments: A Security Analysis of Sudo Session Handling ........................................ 41
Ji Hoon Jeong, Hyung Chan Kim, Il Hwan Park, and Bong Nam Noh

Security of Web of Things: A Survey (Short Paper) ............................. 61
Wei Xie, Yong Tang, Shuhui Chen, Yi Zhang, and Yuanming Gao

Searchable Encryption

UC-Secure Dynamic Searchable Symmetric Encryption Scheme ............. 73
Kaoru Kurosawa, Keisuke Sasaki, Kiyohiko Ohta, and Kazuki Yoneyama

Simple, Secure, and Efficient Searchable Symmetric Encryption with Multiple Encrypted Indexes ......................... 91
Takato Hirano, Mitsuhiro Hattori, Yutaka Kawai, Nori Matsuda, Mitsugu Iwamoto, Kazuo Ohta, Yusuke Sakai, and Tatsuji Munaka

Secure Automata-Based Substring Search Scheme on Encrypted Data ...... 111
Hiroaki Yamamoto

Cryptanalysis

Related-Key Impossible Differential Analysis of Full Khudra ................. 135
Qianqian Yang, Lei Hu, Siwei Sun, and Ling Song

On the Division Property of SIMON48 and SIMON64 .......................... 147
Zejun Xiang, Wentao Zhang, and Dongdai Lin

Practical Analysis of Key Recovery Attack Against Search-LWE Problem . 164
Momonari Kudo, Junpei Yamaguchi, Yang Guo, and Masaya Yasuda
A Note on Fault Attacks Against Deterministic Signature Schemes (Short Paper) .................................................. 182
   Alessandro Barenghi and Gerardo Pelosi

Permutation and Symmetric Encryption

Lower Bounds for Key Length of \( k \)-wise Almost Independent Permutations and Certain Symmetric-Key Encryption Schemes .................. 195
   Akinori Kawachi, Hirotoshi Takebe, and Keisuke Tanaka

Privacy Preserving

Privacy-Preserving Wi-Fi Fingerprinting Indoor Localization ............... 215
   Tao Zhang, Sherman S.M. Chow, Zhe Zhou, and Ming Li

Formal Policy-Based Provenance Audit ...................................... 234
   Denis Butin, Denise Demirel, and Johannes Buchmann

Recipient Privacy in Online Social Networks (Short Paper) .................. 254
   Filipe Beato, Kimmo Halunen, and Bart Mennink

Hardware Security

   Risa Yashiro, Takanori Machida, Mitsugu Iwamoto, and Kazuo Sakiyama

Post-quantum Cryptography

On the Security and Key Generation of the ZHFE Encryption Scheme ...... 289
   Wenbin Zhang and Chik How Tan

Cryptanalysis of a Public Key Cryptosystem Based on Diophantine Equations via Weighted LLL Reduction (Short Paper) ....................... 305
   Jintai Ding, Momonari Kudo, Shinya Okumura, Tsuyoshi Takagi, and Chengdong Tao

Paring Computation

Faster Explicit Formulae for Computing Pairings via Elliptic Nets and Their Parallel Computation..................................................... 319
   Hiroshi Onuki, Tadanori Teruya, Naoki Kanayama, and Shigenori Uchiyama

Author Index ............................................................................. 335
Advances in Information and Computer Security
11th International Workshop on Security, IWSEC 2016,
Tokyo, Japan, September 12-14, 2016, Proceedings
Ogawa, K.; Yoshioka, K. (Eds.)
2016, XII, 335 p. 64 illus., Softcover
ISBN: 978-3-319-44523-6